世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G09C 1/00, H04L 9/32	A1	(11) 国際公開番号	WO99/12144
		(43) 国際公開日	1999年3月11日(11.03.99)

(21) 国際出願番号 PCT/JP98/03888

(22) 国際出願日 1998年9月1日(01.09.98)

(30) 優先権データ
特願平9/236926 1997年9月2日(02.09.97) JP
特願平9/236927 1997年9月2日(02.09.97) JP

(71) 出願人（米国を除くすべての指定国について）
株式会社 キャディックス(CADIX INC.)[JP/JP]
〒154-0014 東京都世田谷区新町2丁目26番15号
Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
田吹隆明(TABUKI, Takaaki)[JP/JP]
〒154-0014 東京都世田谷区新町2丁目26番15号
株式会社 キャディックス内 Tokyo, (JP)
(74) 代理人
弁理士 吉田研二, 外(YOSHIDA, Kenji et al.)
〒180-0004 東京都武蔵野市吉祥寺本町1丁目34番12号
Tokyo, (JP)

(81) 指定国 AU, BR, CA, CN, KR, NZ, RU, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

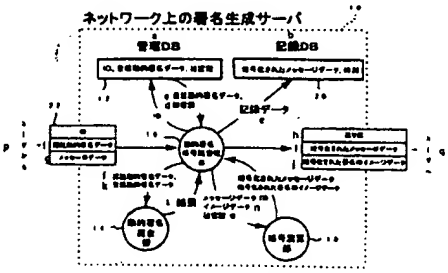
添付公開書類
国際調査報告書

(54)Title: DIGITAL SIGNATURE GENERATING SERVER AND DIGITAL SIGNATURE GENERATING METHOD

(54)発明の名称 ディジタル署名生成サーバ及びディジタル署名生成方法

(57) Abstract

A digital signature system using a public key code method in which the management of a private key is easy and the convenience is enhanced. A dynamic signature encryption key management unit (16) obtains registered dynamic signature data and a private key from a management database (12) in accordance with an "ID" transmitted from a user. The registered dynamic signature data and authentication dynamic signature data transmitted from the user are collated with each other by a dynamic signature collation unit (14). If both the data are judged to be identical, the dynamic signature encryption key management unit (16) supplies message data transmitted from the user and the private key to an encryption calculation unit (18), which transmits the message data etc. encrypted by the private key to the dynamic signature encryption key management unit (16). The dynamic signature encryption key management unit (16) transmits the message data etc. which are encrypted, i.e. signed, back to the user. It is not necessary for the users to manage their own private keys by themselves, so that a digital signature system significantly convenient can be obtained.



DERWENT-ACC-NO: 1999-214793

DERWENT-WEEK: 200217

TITLE: Digital signature generation server for data encryption

INVENTOR: TABUKI, T

PATENT-ASSIGNEE: CYBER SIGN JAPAN INC[CYBEN] , CADIX INC[CADIN] , CADIX KK[CADIN]

PRIORITY-DATA: 1997JP-0236927 (September 2, 1997) , 1997JP-0236926 (September 2, 1997)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
WO 9912144 A1	March 11, 1999	J	049	G09C 001/00
AU 742717 B	January 10, 2002	N/A	000	G09C 001/00
JP 11088321 A	March 30, 1999	N/A	013	H04L 009/32
JP 11088322 A	March 30, 1999	N/A	010	H04L 009/32
AU 9888883 A	March 22, 1999	N/A	000	N/A
EP 1030282 A1	August 23, 2000	E	000	G09C 001/00
CN 1272934 A	November 8, 2000	N/A	000	G09C 001/00
KR 2001023602 A	March 26, 2001	N/A	000	G09C 001/00
BR 9811737 A	November 20, 2001	N/A	000	G09C 001/00

DESIGNATED-STATES: AU BR CA CN KR NZ RU SG US AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE DE FR GB IT

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
WO 9912144A1	N/A	1998WO-JP03888	September 1, 1998
AU 742717B	N/A	1998AU-0088883	September 1, 1998
AU 742717B	Previous Publ.	AU 9888883	N/A
AU 742717B	Based on	WO 9912144	N/A
JP 11088321A	N/A	1997JP-0236926	September 2, 1997
JP 11088322A	N/A	1997JP-0236927	September 2, 1997
AU 9888883A	N/A	1998AU-0088883	September 1, 1998
AU 9888883A	Based on	WO 9912144	N/A
EP 1030282A1	N/A	1998EP-0940645	September 1, 1998
EP 1030282A1	N/A	1998WO-JP03888	September 1, 1998
EP 1030282A1	Based on	WO 9912144	N/A
CN 1272934A	N/A	1998CN-0809775	September 1, 1998
KR2001023602A	N/A	2000KR-0702250	March 2, 2000
BR 9811737A	N/A	1998BR-0011737	September 1, 1998
BR 9811737A	N/A	1998WO-JP03888	September 1, 1998
BR 9811737A	Based on	WO 9912144	N/A

INT-CL (IPC): A61B005/117, G06T007/00 , G09C001/00 , H04L009/32

ABSTRACTED-PUB-NO: WO 9912144A

BASIC-ABSTRACT:

NOVELTY - A digital **signature server** has a dynamic signature encryption key management unit which obtains registered dynamic signature data and a private key from a management database in accordance with an ID transmitted from a

user. The registered dynamic signature data and authentication dynamic signature data transmitted from the user are collated with each other by a dynamic signature collation unit. If both the data are judged to be identical, the key management unit supplies message data transmitted from the user and the **private key** to an encryption calculation unit, which transmits the message data etc. encrypted by the **private key** to the key management unit which transmits the message data etc. which are encrypted, i.e. **signed,** back to the user.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for a digital signature generating method.

USE - For data encryption.

ADVANTAGE - It is not necessary for the users to manage their own private keys by themselves, thus is more convenient.

CHOSEN-DRAWING: Dwg.0/7

TITLE-TERMS: DIGITAL SIGNATURE GENERATE SERVE DATA ENCRYPTION

DERWENT-CLASS: P31 P85 W01

EPI-CODES: W01-A05B;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N1999-158102